REMARKS/ARGUMENTS

The present amendment is responsive to the final Office Action dated February 28, 2007. Claims 1, 19, 36 and 46 have been amended. No new matter has been introduced by these amendments, support for which may be found, by way of example only, in substitute specification paragraphs 0472-0483 and in FIGS. 4-7 and 22-23. Claims 180 and 182 have been cancelled. Thus, claims 1, 4-9, 12-16, 19, 22-26, 29-33, 36, 39-43, 46, 179 and 181 are again presented for consideration in view of the following remarks. A petition for a 1-month extension of time is submitted along with a Request for Continued Examination. The pending rejections will be addressed in view of the claims as currently presented.

Reexamination and reconsideration of the above- identified application, pursuant to and consistent with 37 C.F.R. § 1.116, and in light of the remarks that follow, are respectfully requested. Because the present claims are believed to be in condition for allowance over the cited art, good cause exists for the entry of this reply in accordance with 37 C.F.R. § 1.116.

Claims 1, 4, 7, 12, 16, 19, 22, 24, 29, 33, 36, 39, 41 and 46 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,253,193 ("*Ginter*"). Applicants respectfully traverse the rejection.

The present invention has been extensively discussed in the prior amendments and replies, which are incorporated by reference for brevity. As independent claims 1, 19, 36 and 46 are currently amended, the features of those claims as presently presented will be addressed below.

Independent claim 1 has been amended to recite "A data processing apparatus for processing content data provided by a recording or communication medium, said apparatus comprising: a cryptography process section for executing a cryptography process on said content data; and a control section for executing control for said cryptography process section, wherein said cryptography process section is configured to: split a first portion of header data of the content data having data on usage policy into a plurality of first messages, said header data including a first stored check value therein, generate a first integrity check value or values from a first key stored in said cryptography process section to verify integrity of the header data by using said plurality of first messages, collate said first integrity check value or values to verify said first portion of the header data including the usage policy by comparing said first integrity check value or values to said first stored check value, split a second portion of the header data of

the content data having a content key into a plurality of second messages, said header data including a second stored check value therein, generate a second integrity check value or values from a second key stored in said cryptography process section to verify integrity of the header data by using said plurality of second messages, collate said second integrity check value or values to verify said second portion of the header data including a block information table by comparing said second integrity check value or values to said second stored check value, generate an intermediate integrity check value based on said first integrity check value or values and said second integrity check value or values, and use said intermediate integrity check value to verify said content data corresponding to said first and second integrity check values."

Independent claim 19 has been amended to recite "A data processing method for processing content data provided by a recording or communication medium, said method comprising: splitting a first portion of header data of the content data having data on usage policy into a plurality of first messages, said header data including a first stored check value therein; generating first integrity check value or values from a first key to verify integrity of the header data by using said plurality of first messages; collating said first integrity check value or values to verify said first portion of the header data including the usage policy by comparing said first integrity check value or values to said first stored check value; if said first portion of the header data is verified, splitting a second portion of the header data of the content data having a content key into a plurality of second messages, said header data including a second stored check value therein; generating second integrity check value or values from a second key to verify integrity of the header data by using said plurality of second messages; collating said second integrity check value or values to verify said second portion of the header data including a block information table by comparing said second integrity check value or values to said second stored check value; if said second portion of the header data is verified, generating an intermediate integrity check value based on said first integrity check value or values and said second integrity check value or values; and verifying said content data corresponding to said first and second integrity check values using said intermediate integrity check value.

Independent claim 36 has been amended to recite "A data verifying value imparting method for a data verifying process, said method comprising: splitting a first portion of header data of data having data on usage policy into a plurality of first messages, said header data including a first stored check value therein; imparting first integrity check value or values by using said plurality of first messages; comparing said first integrity check value or values to

said first stored check value to verify a usage policy of said header data; if said usage policy is verified, splitting a second portion of the header data of the data having a content key into a plurality of second messages, said header data including a second stored check value therein; imparting second integrity check value or values by using said plurality of second messages; comparing said second integrity check value or values to said second stored check value to verify a block information table of said header data; and if said block information table is verified, imparting an intermediate integrity check value to data to be verified, said intermediate integrity check value being used to verify content data corresponding to said first integrity check value or values and said second integrity check value or values."

And independent claim 46 has been amended to recite "A recording medium recorded with a computer program for executing a data verifying process having certain actions, said actions comprising: splitting a first portion of header data of data having data on usage policy into a plurality of first messages, said header data including a first stored check value therein; executing a collation process using a first integrity check value or values generated by using said plurality of first messages, including comparing said first integrity check value or values to said first stored check value to verify a usage policy of said header data; if said usage policy is verified, splitting a second portion of the header data of the data having a data key into a plurality of second messages, said header data including a second stored check value therein; executing a collation process using a second integrity check value or values generated by using the plurality of second messages, including comparing said second integrity check value or values to said second stored check value to verify a block information table of said header data; and if said block information table is verified, using an intermediate integrity check value to verify said content data corresponding to said first and second integrity check values, said intermediate integrity check value being based on an integrity check value set obtained by combining at least some of said first and second integrity check values together."

Applicants respectfully submit that *Ginter* does not teach or suggest each and every limitation of these independent claims. For instance, each of claims 1, 19, 36 and 46 requires header data including first and second stored check values stored therein. The example shown in FIG. 4 of the instant application illustrates that the header section includes an integrity check value A (ICVa) as well as an integrity check value B (ICVb).

In contrast, applicants submit that *Ginter* does not disclose such a configuration. Rather, as shown in FIG. 17 of *Ginter*, there may be a public header 802 and a private header

804 as well as separate permission records 808 in an electronic container 302. And in a given permission record 808, there is a header section 900 and a control set record, as shown in FIG. 26A. Even assuming that *Ginter's* check value 978 or check value 980 of FIG. 26A or the check value 994 of FIG. 26B were equivalent to the claimed integrity check values, which applicants do not believe is the case, *Ginter's* check values are not stored in either header 900 of FIG. 26A or header 908a of FIG. 26B.

Furthermore, claims 1 and 19 require generating a first integrity check value from a first key and generating a second integrity check value from a second key. The first integrity check value is collated to verify a usage policy associated with a first portion of the header data by comparing the first integrity check value to the first stored check value. And the second integrity check value is collated to verify a block information table associated with a second portion of the header data by comparing the second integrity check value to the second stored check value. According to applicants' understanding of *Ginter*, the reference neither teaches nor suggests such operation.

Claims 36 and 46 are similar to claims 1 and 19 in that there is a comparison between the first integrity check value to the first stored value to verify a usage policy of the header data. Claims 36 and 46 also require a comparison between the second integrity check value to the second stored value to verify a block information table of the header data. This latter comparison occurs if the usage policy is verified. Such operation is illustrated in the exemplary flow chart of FIG. 22 of the instant application. Claims 36 and 46 also include that if the block information table is verified, then an intermediate integrity check value is imparted to data to be verified (claim 36) or the intermediate integrity check value is used to verify the content data corresponding to the first and second integrity check values (claim 46). Applicants submit that *Ginter*, as best understood, does not disclose such limitations.

For at least these reasons, applicants respectfully submit that independent claims 1, 19, 36 and 46 are not anticipated by *Ginter* and the rejection of claims 1, 19, 36 and 46 should therefore be withdrawn. Claims 4, 7, 12, 16, 22, 24, 29, 33, 39, and 41 depend from claims 1, 19 and 36, respectively, and contain all of the limitations thereof. Accordingly, for at least this reason, applicants submit that these dependent claims are likewise patentable.

Claims 5, 6, 23 and 40 were rejected under 35 U.S.C. § 103(a) as being obvious over *Ginter* in view of U.S. Patent 6,898,709 ("*Teppler*"). Claims 8, 25 and 42 were rejected under 35 U.S.C. § 103(a) as being obvious over *Ginter* in view of U.S. Patent 6,011,849

("*Orrin*"). Claims 9, 26 and 43 were rejected under 35 U.S.C. § 103(a) as being obvious over *Ginter* in view of *Orrin* and U.S. Patent 6,915,434 ("*Kuroda*"). And claims 13-15 and 30-32 were rejected under 35 U.S.C. § 103(a) as being obvious over *Ginter* in view of U.S. Patent 6,253,193 ("*Bodo*"). Applicants respectfully traverse each of these § 103(a) rejections.

Claims 5, 6, 8, 9, 13-15, 23, 25, 26, 30-32, 40, 42, and 43 depend from independent claims 1, 19 and 36, respectively, and contain all the limitations thereof. Thus, for at least this reason, applicants submit that the subject dependent claims are likewise patentable.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicants' attorney at (908) 654-5000 in order to overcome any additional objections which he might have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: June 28, 2007   Respectfully submitted,

By _____
Andrew T. Zidel
  Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
  KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant

780264_1.DOC